PAUL GRANT
LAW OFFICE OF PAUL GRANT
P.O. Box 2720
Parker CO 80134
303-909-6133

February 5, 2018

BY ECF
Hon. Katherine B. Forrest
United States District Judge
United States District Court
500 Pearl Street
New York NY 10007

Re: *United States v. Ross William Ulbricht, et al*, 14 Cr. 68 (KBF)
Request to Partially Unseal and Make Available to Counsel and Defendant Three Magistrate's Files

Dear Judge Forrest:

I write on behalf of Defendant Ross Ulbricht to request that three SDNY magistrate's files (13 MAG 2258, 13 MAG 2274, 13 MAG 2275) be partially unsealed and that the entire contents of those files be made available to counsel for the parties and to Mr. Ulbricht, for examination and review and use in this case. I have contacted the government about this request, and AUSA Eun Young Choi advises the government will oppose this request.

As the court may recall from pre-trial suppression proceedings, the government obtained five pen-trap orders authorizing the pen register and trap and trace collection of data sent to and from Ulbricht's router or to and from a device (assumed to be Ulbricht's computer) associated with a particular MAC address, including: 13 MAG 22, a Sealed Order for the Secret Service, directed to Comcast to provide assistance; 13 MAG 2228, a Sealed Order for the Secret Service, directed to Comcast to provide assistance; 13 MAG 2258 (the 9.19.13 wireless router pen for FBI); 13 MAG 2274 ((9.20.13.Router Pen for FBI); and 13 MAG 2275 (9.20.13.MAC Address Pen for FBI). Doc. 48, Memorandum of Law in Support of Defendant Ross Ulbricht's Pre-Trial Motions to Suppress Evidence . . ., at pages 37 -39 (page numbers in original document).

The latter three orders, each of which is directed to the FBI (the "three FBI pen-trap orders"), were issued in the three sealed magistrate's files (13 MAG 2258, 13 MAG 2274, 13 MAG 2275) which Mr. Ulbricht now wishes to examine.

Mr. Ulbricht argued in his motion to dismiss that the data collection resulting from the five pen-trap orders must be suppressed because this data collection required search warrants based on probable cause, and because the orders failed to adhere to statutory limitations. See

Doc. 48, Memorandum of Law in Support of Defendant Ross Ulbricht's Pre-Trial Motions to Suppress . . ., at page 37. Mr. Ulbricht's pre-trial Motion to Suppress was hampered by the fact that the government had not disclosed the pen-trap data it had (allegedly) collected. Because the government failed to disclose all of the pen-trap data, Mr. Ulbricht could only attack the scope of the pen-trap orders, *i.e*., what they authorized. Mr. Ulbricht was not able to separately attack, for example, whether the government's collection actually complied with the statute and with the terms of the pen-trap orders.

In a pre-trial discovery request, Mr. Ulbricht had requested from the government *any and all data obtained from pen registers judicially authorized in this case*. Doc 70-3, par. 13, p. 3, letter from J. Dratel to AUSA S. Turner, et al.

The government responded to that defense discovery request:

The Government has provided all available pen register data used to detect Ulbricht's email and Internet activity in September 2013, as well as pen register data received from Icelandic law enforcement authorities concerning the SR Server and the server described in the Tarbell Declaration as Server-1. To the extent any other pen register information was obtained in the course of the investigation, the Government objects to this request on the ground that such information is not material to the defense or otherwise required to be produced under Rule 16. See Doc 70-4 at p. 5, 9/23/2014 letter from AUSA Serrin Turner to Joshua Dratel.

In this response to the defense discovery request, the government stated that it had provided *all available pen register data* used to detect Ulbricht's email and internet activity in September 2013, but *the government did not state that it had actually produced anything, or if it did, what other data was not available*. That appears to have been a false or at best ambiguous statement unless some of the relevant collected data was then unavailable, *because the government did not, in fact, provide the pen-trap data referred to in the laptop search warrant affidavit.* See below.

The only pen-trap data provided to the defense before trial was data that appears to have resulted from collection authorized in the 9/17/2013 Pen Trap Order in Case No. 13 MAG 2236. Declaration of Paul Grant In Support of Partial Unsealing, at par. 5-7. That order authorized a trap and trace device to identify the IP address of internet communications directed to, and a pen register to determine the destination IP addresses of, any Internet communications originating from the "Target Account," referring to a Comcast account.

Mr. Ulbricht has still not received the data resulting from the three FBI pen-trap orders identified above. The government relied on the data supposedly obtained from those pen-trap orders, to monitor Ulbricht's online activity, to correlate his activity to that of DPR, and to establish, in the minds of investigators, that Ulbricht was DPR. Those are the facts testified to in the laptop search warrant affidavit, facts used to establish probable cause for the laptop search warrant to issue.

In the laptop search warrant affidavit, the affiant, Christopher W. Tarbell, FBI Special Agent, testified, in relevant part:

> 5. . . . The computer contains a network adapter assigned the MAC address 88-53-2E-9C-81-96.
>
> **PROBABLE CAUSE**
> **OVERVIEW**
> **IDENTIFICATION OF "DREAD PIRATE ROBERTS"**
> **AS ROSS WILLIAM ULBRICHT**
> **ULBRICHT'S USE OF THE SUBJECT COMPUTER**
>
> . . .
>
> 35. On September 20, 2013, the Government obtained a judicial order authorizing the FBI to use a pen register/trap and trace device . . . Data obtained from the Wireless Router Pen-Trap the same day showed a computer with the MAC address 88-53-2E-9C-81-96 - that is, the SUBJECT COMPUTER - regularly accessing the router.
>
> 36. Based on my training and experience . . . I determined that the manufacturer associated with the MAC address of the subject computer produces network cards for computers running the Windows operating system. The Subject Computer is the only Windows-based computer that has been detected from the Wireless Routing Pen . . .
>
> 39. On September 20, 2013, the FBI collected data from the Wireless Router Pen-Trap over the course of several hours, which showed the SUBJECT COMPUTER logging on and off the wireless router at the Subject Residence at the same time that DPR logged on and off of Pidgin.
>
> 40. On September 20, 2013, the Government obtained a judicial order authorizing the FBI to use a pen register/trap and trace device . . . to collect routing data . . .
>
> 41. This surveillance yielded the following results:
>
> a. At approximately 11:15 a.m., PDT, pen register data from the Subject Computer Pen-Trap showed the Subject Computer logging onto the internet at the Subject Residence . . .
>
> 42. Based on the foregoing, I respectfully submit there is probable cause to believe that Ulbricht uses the SUBJECT COMPUTER and that he specifically uses it in connection with his operation of Silk Road.

Excerpts from Laptop Search Warrant.

Paragraphs 35, 39, and 41 refer to the FBI pen-trap orders, from which no data has ever been produced to the defense. Paragraph 42 in the affidavit shows the government relied on the pen-trap data described above, data resulting from the three FBI pen-trap orders, to establish probable cause to obtain the laptop search warrant.

The data collected pursuant to the three FBI pen-trap orders should be contained in the 3 magistrate's files (13 MAG 2258, 13 MAG 2274, 13 MAG 2275). See 18 U.S.C. § 3123. Mr. Ulbricht is requesting the magistrates' files be partially unsealed and the contents made available to counsel for both parties and to the defendant, because these files should contain the following material and discoverable information:

a record which will identify (I) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network; (ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information; (iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and (iv) any information which has been collected by the device. 18 U.S.C. § 3123. "The record to be maintained must be provided *ex parte* and under seal to the court which authorized the installation and use of the device within 30 days after termination of the order." *Id*.

Mr. Ulbricht is entitled to examine the contents of the three magistrate files, to see if what the government claimed to have collected was collected, and to see how the data was collected. To withhold that data now would be unconscionable. That information was material to preparation by the defense, was in the possession of the FBI, both before and after the deadline by which the law required it to have been filed with the magistrates, and it should have been disclosed to the defense prior to trial. Rule 16(a)(1)(E)(I), Fed.R.Crim.P. The government told the court that these pen registers were not used to geo-locate Mr. Ulbricht - apparently without having access to the data collected pursuant to the three FBI pen-trap orders. Doc. 57, Tarbell Declaration at Page 9 of 10, par. 21. These files should help address that issue.

The government has never produced the data collected pursuant to four out of the five pen-trap orders, yet argued before trial against suppression of evidence obtained from the pen registers on the basis of the government's representation as to what each of the pen registers did and did not collect. If the government did not have the data, then providing the court with statements from the affidavit of an FBI special agent who should have provided them with the data itself, was incautious. If the government had the data, but did not produce it upon request, and misrepresented what the data contained in argument to the court, that would be a serious problem; if the government had the data but simply did not produce it, that would constitute a serious discovery violation.

The government stated that the pen registers were used to establish when Ulbricht logged

onto and off of the internet, in defending the search warrant, in support of their argument that the search warrant applications to search for information to allow comparison with online activity were reasonable requests seeking relevant information, referencing Tarbell Decl. Ex. M., par. 33-41. See Doc. 56 at 29.

Mr. Ulbricht has discovered new information, information which has just recently become available, that reveals that the government did use electronic surveillance to track his location, at the very same time, and as part of, its pen register data collection. The government apparently used its WiFi sniffing and tracking surveillance (as part of the pen-trap data collection) to track and determine Ulbricht's precise location, and to determine when he logged in and out on his laptop, while Ulbricht was in his residence. This information is provided in the the book titled *American Kingpin*, a book published in May 2017, long after the trial was concluded.

According to the author, Nick Bilton, his accounts are based, in part, on more than 250 hours spent with federal agents involved in the investigation, including FBI special agents [Tarbell and Kiernan], and including Homeland Security special agent Jared Der-Yeghiayan. Bilton's account of FBI surveillance correctly places Tarbell, Der-Yeghiayan, and Kiernan on site outside Ulbricht's residence, a short time before Ulbricht's arrest. He describes the actions and observations of these agents, in considerable detail and in credible terms, in a manner consistent with material previously disclosed by the government.

Bilton describes the FBI surveillance of Ulbricht in his residence:

"Jared [Der-Yeghiayan], Thom [Thomas Kiernan], and Brophy stood in front of the café near Ross' house, listening to Tarbell . . . They knew that Ross was at home because the FBI had an undercover SUV circling his block and monitoring the Wi-Fi traffic (this is pen register and trap and trace activity). The system they were using (which should be described in the magistrates' files) would check the signal strength of the Wi-Fi on his computer and then, by triangulating that data from three different points they had captured as they drove around the block, they were able to figure out Ross's exact location, which at this very moment was his bedroom, on the third floor of his Monterey Boulevard apartment." Bilton at 331.

Under Federal Rule of Criminal Procedure 16(a)(1)(E), the government is required to produce documents or data "if the item is within the government's possession, custody, or control and . . . the item is material to preparing the defense." Rule 16(a)(1)(E) permits discovery related to the constitutionality of a search or seizure. *U.S. v. Hector Soto-Zuniga*, 837 F.3d 992, 1003 (9th Cir. 2016). Materiality is a " low threshold; it is satisfied so long as the information . . . would have helped" to prepare a defense. *Id., quoting United States v. Hernandez-Meza*, 720 F.3d 760, 768 (9th Cir. 2013).

The defendant was entitled to rely on the government's statement that it had provided all available pen-trap data related to monitoring Ulbricht's internet activity, and on the statement

that any other pen-trap data it may have was not material and not subject to production. *See United States v. Lee*, 573 F.3d 155, 161 (3d Cir. 2009).

It appears the government may now have the PRTT data that the FBI collected in September 2013 pursuant to the three FBI pen-trap orders. Declaration of Paul Grant In Support of Partial Unsealing, par. 10. Any relevant PRTT data the FBI had collected in 2013 was required by statute to have been placed in the three magistrate's files. That PRTT data in the magistrate's files may well be more extensive than the new PRTT data (or may not even include the same data) that the government is now prepared to disclose, and is data that would have been in possession of the FBI pre-trial in 2014, when the defense requested it. Any and all such data should have been provided to the defense prior to trial. That data was material and relevant to preparing the defense, particularly because the pen-traps were directly at issue.

The prosecutor is obligated to disclose to the defendant evidence which is favorable to the defense and suppression of the evidence which is material to either guilt or punishment, violates due process, regardless of the good faith or the bad faith of the prosecutor. *Brady v. Maryland*, 373 U.S. 83, 86-88. (1963). *Brady* itself is a case involving a post-conviction claim of newly discovered evidence. *See Id.*, at 85. "Society wins not only when the guilty are convicted but when criminal trials are fair; our system of the administration of justice suffers when any accused is treated unfairly." *Id.*, at 88.

It is clear that the government did not produce in discovery prior to trial the data that is, or should be, in the three magistrate's files; it appears that the government violated its disclosure obligations under Rule 16 and under *Brady*, and the defense has reason to believe that the evidence it failed to disclose will prove to be exculpatory.

Mr. Ulbricht was unable to review the data before trial, the pen-trap data upon which the government relied to establish probable cause for issuance of both the laptop and residence search warrants. Mr. Ulbricht was, therefore, denied his due process right to effectively challenge the constitutionality of the laptop and residence search warrants. The best way to begin to remedy that violation now, is to allow Mr. Ulbricht to access the data that the government improperly withheld prior to trial, PRTT data which by law should be located in the three magistrate's files.

PRTT evidence withheld in violation of Rule 16 discovery obligations or in violation of *Brady* obligations before trial, will be newly discovered evidence now. Mr. Ulbricht requires access to the material in the three magistrate's files, to determine whether that data is newly discovered evidence which will support his Rule 33 Motion for a New Trial.

The prosecutor should join in this motion, not oppose it. "The United States Attorney is the representative . . . of a sovereign whose obligation to govern impartially is as compelling as its obligation to govern at all; and whose interest, therefore, in a criminal prosecution is not that it shall win a case, but that justice shall be done." *Berger v. United States*, 295 U.S. 78, 88

(1935). Prosecutors have an ethical duty to reveal exculpatory evidence obtained after conviction. See ABA Model Rules of Professional Conduct, Rule 3.8(g) (2012). If the prosecutor opposes this motion, as they have stated they will, they will be supporting their own improper withholding of evidence prior to trial, and they will be supporting the misleading or misinformed statements they made to the defendant and the court.

Post-conviction judicial decisions should be made with the sole purpose of insuring justice. *See Imbler v. Poachtman*, 424 U.S. 409, 428 (1976). Mr. Ulbricht is serving a sentence to life without parole and under such dire circumstances, justice requires that this court order that the contents of the sealed magistrate's files be made available to counsel for both parties and to the defendant.

WHEREFORE, for all the reasons provided above, and in the interests of justice, Mr. Ulbricht requests that the court order the partial unsealing of three magistrate's files, namely files identified as 13 MAG 2258, 13 MAG 2274, 13 MAG 2275, and that the contents of those three files be made available for examination and review, to counsel for both parties and to the defendant. Mr. Ulbricht also requests such additional relief as the court finds to be just and equitable.

Respectfully submitted,

/s/ Paul Grant
Paul Grant
Counsel for Ross William Ulbricht

cc: Eun Young Choi (by ECF)
Assistant United States Attorney